System Protection Profile - Industrial Control Systems

Version 0.91

February 4, 2004

Prepared for:

by

Document Control

Preparation

Action	Name	Date
Prepared by:	Ron Melton, Terry Fletcher, Matt Earley	4 Feb 2004
Reviewed by:	Lynne Ambuel, Murray Donaldson	4 Feb 2004

Release

Version	Date Released	Change Notice	Pages Affected	Remarks
0.91	4 Feb 2004	N/A	All	SPP populated into new structure. Core information chapters (1 to 6) nearing completion. Chapters 7 and 8 (Application Notes & Rationale) under development.

Distribution List

Name	Organisation	Title
Keith Stouffer	NIST	PCSRF Program Manager
PCSRF Members	Various	Various

TABLE OF CONTENTS

LIST OF TABLES

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this System Protection Profile are consistent with those used in Version 2.1 of the Common Criteria [CC]. Selected presentation choices are discussed here to aid the System Protection Profile reader. The CC allows several operations to be performed on functional requirements: The allowable operations defined in paragraph 2.1.4 of Part 2 of the CC [CC2] are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].

- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text.**

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.

- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

All operations described above are used in this System Protection Profile. *Italicized text* is used for both official document titles and text meant to be emphasized more than plain text.

Terminology

The terminology used in the System Protection Profile is that defined in the Common Criteria [CC1, CC2]. A glossary has also been provided in Appendix A – Acronyms.

References

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999.

[CC1] Common Criteria Part 1: Introduction and General Model, Version 2.1, CCIB-99-031, August 1999.

[CC2] Common Criteria Part 2: Security Functional Requirements, Version 2.1, CCIB-99032, August 1999.

[CC3] Common Criteria Part 3: Security Assurance Requirements, Version 2.1, CCIB-99033, August 1999.

[CEM] Common Evaluation Methodology Part 2: Evaluation Methodology, Version 1.0, CEM99/045, August 1999.

Document Organization

Section 1 provides the introductory material for the System Protection Profile.

Section 2 provides general purpose and STOE description.

Section 3 provides a discussion of the expected environment for the STOE. This section also defines the set of threats that are to be addressed by either the technical, operational or management controls implemented by the STOE or through the environmental controls.

Section 4 identifies the risks to the STOE that have been derived from the statement of the security environment defined in section 3.

Section 5 defines the security objectives for both the STOE and the STOE environment.

Section 6 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3 [CC2, CC3], respectively that must be satisfied by the STOE.

Section 7 contains guidance information for SST authors who would like to claim conformance to the SPP.

Section 8 provides a rationale to explicitly demonstrate that the identified risks to the STOE have been derived from the aspects identified in the security environment. It also demonstrates how the security objectives have been derived from each of the identified risks. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Section 8 also provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the System Protection Profile requirements.

Appendix A documents an acronym list to define frequently used acronyms applicable to the STOE.

1 Introduction

This introductory section presents *System Protection Profile (SPP)* identification information and an overview of the SPP.

1.1 SPP Identification

This section provides information needed to identify and control this SPP. This SPP targets an **extended Evaluation Assurance Level (EAL) 3** level of assurance for the STOE.

SPP Title:	System Protection Profile - Industrial Control Systems
SPP Version:	0.91
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.1 Final
SPP Evaluation:	National Information Assurance Partnership
Author(s):	National Institute of Standards & Technology
Keywords:	Industrial Control Systems

1.2 SPP Overview

SPP Background

This SPP has been developed as part of the Process Control Security Requirements Forum (PCSRF) sponsored by the National Institute of Standards and Technology (NIST). This SPP is intended to provide an ISO 15408 based starting point in formally stating security requirements associated with industrial control systems (ICS). This SPP includes security functional requirements (SFRs) and security assurance requirements (SARs) that extend ISO 15408 to cover issues associated with systems. These extensions are based on current ISO subcommittee work to extend ISO 15408 to cover the accreditation of systems and the evaluation of system protection profiles and system security targets. These extensions broaden consideration of security controls to include non-technical controls based on procedural and management functions.

ICS Background

Industrial control systems are computer-based systems used to control industrial processes and physical functions. This SPP covers the security requirements for a generic ICS. The SPP has been written in such a way that it may be used as the basis for preparing a System Security Target for a specific ICS or as the basis for a more detailed SPP for a sub-class of ICS such as a Supervisory Control and Data Acquisition System (SCADA). For more discussion of the role of this SPP refer to section 7.1 of the application notes.

Modern industry and the associated infrastructure is based on our ability to control electrical, chemical and mechanical transformations of materials to produce desired results. Industrial control systems are used to automate these control functions allowing the creation of industrial processes that are faster, larger and more complex than could be achieved by non-automated means. In many cases the ICS is also an integral element of the safe and environmentally acceptable operation of the industrial process.

There are several varieties of ICS, but all consist of the same basic elements. As shown in Figure 1 those components are: the controller, sensors, actuators (or final control elements), and in some cases a human machine interface (HMI) and a remote diagnostics and maintenance capability. These components may be in close physical proximity or they may be distributed with great distances (many miles) between some of the elements) depending on the specific application. In addition to these technical elements ICS include a human element including operators, maintainers and engineers. They also have operating procedures and other non-technical elements.

A simplified view of the operation of an ICS and the function of the elements is as follows. The controller implement control algorithms based on a mathematical model of the process to be controlled and the control objectives. The sensors sense the state of the process through measurement of process parameters such as temperature, pressure, voltage, pH, position, size, etc. The state of the process may change due to external "disturbances", changes in the process inputs such as feed material, or in response to action initiated by the controller. The controller processes the sensor information and, based on the control algorithm and desired state of the process, sends commands to the final control elements which in turn interact with the controlled process to affect changes in its state. The final control elements take many different forms including valves, switches, relays, motors, and so forth depending on the nature of the process under control. The HMI provides a means for human operators to monitor the state of the process and the ICS, to interact with the controller to change the control objective and may also include manual control options. Similarly there may be a remote diagnostics and maintenance interface to be used in gathering data used for diagnostics and maintenance or for other similar activities.

Need for an ICS SPP

Several factors have raised concern about the security of industrial control systems. First, there has been a general trend to replace specialized control devices, particulalry controllers and communications elements, with general purpose computer equipment and associated data communications technology. Second, many companies have chosen to interconnect their process control networks with their corporate intranet once they have introduced general-purpose equipment into the process control system. These two factors introduce all of the potential vulnerabilities found in the network computing in general, particularly if there is a path through the corporate intranet to the Internet at large. Third, for ICS that are broadly distributed a variety of communications media are used including the public switched telephone system, wireless communications and the Internet. There are potential security vulnerabilities associated with each of these communications paths. Finally, ICS are key components of much of our national critical infrastructure including the electric power, water and water treatment, oil and gas production and distribution as well as industrial and military manufacturing.

To address these vulnerabilities organizations are primarily installing security retrofits or upgrades to existing their existing ICS. This SPP is intended to provide a basis for these activities as well as the design of new systems. In either case, the security functionality should be implemented based on a risk analysis that determines security requirements based on an assessment of threats, vulnerabilities and impacts.

System Protection Profile - Industrial Control Systems

The System Protection Profile for Industrial Control Systems (SPP-ICS) specifies the integrated set of security requirements for industrial control systems. The integrated set of requirements includes requirements for operating policies and procedures, requirements for information technology based system components, requirements for interfaces and interoperability between system components, and requirements for the physical environment and protection of the system.

Because the SPP-ICS represents an integrated view of the requirements, special consideration is given to decomposition of security functionality and assignment of specific security functions to sub-systems or components of the overall integrated system. Likewise, the decomposition or composability of the security functionality is also considered. The goal of this aspect of analysis and design is to define security requirements for subsystems or system components at the lowest possible level while at the same time retaining the required level of assurance and security functionality for the integrated system as a whole.

As shown in Figure 1 an industrial control system consists of classes of components for the direct control of a process (the controller(s), actuators and sensors) a human machine interface and capabilities for remote diagnostics and maintenance. Although not represented in the diagram, there are also human elements such as operators and non-techical elements such as operating procedures.

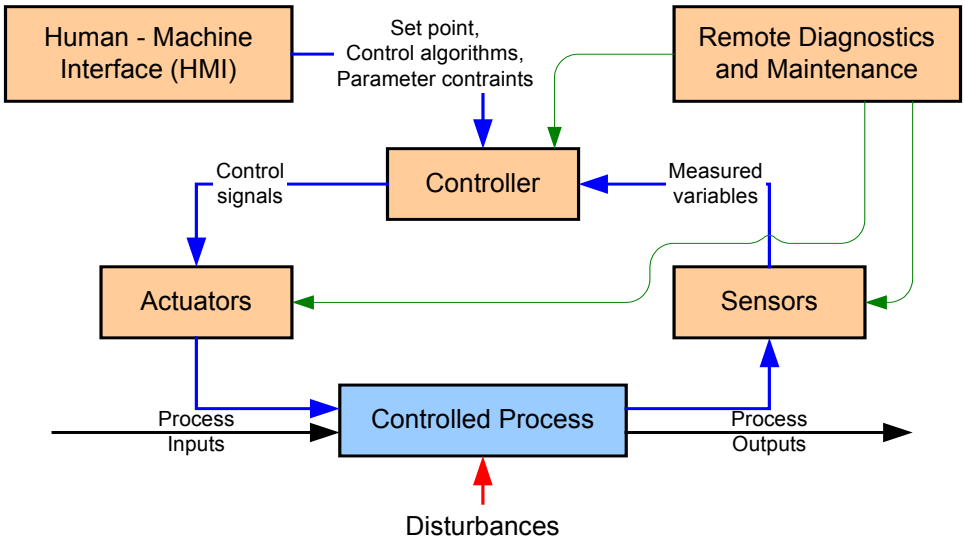

Figure 1: Generic industrial control system

This system protection profile is written for a generic industrial control system as a high-level statement of requirements. It provides a starting point for more specific and detailed statements of requirements for industrial control systems focused on a specific industry, company, or component.

2 STOE Description

This section provides context for the STOE evaluation by identifying the system and describing the evaluated configuration.

2.1 Overview of the System Target of Evaluation (STOE)

This section describes the security subsystem of the industrial control system. The security subsystem includes both the information technology based components and the non-information technology based elements implemented via policies and operating procedures. Particular attention is given to the interaction and dependencies between the security subsystem and the overall industrial control system.

The STOE focuses on protecting data integrity and system availability without interfering with safety system functions. Data integrity centers on protecting data flows to and from the controller and the other ICS components or subsystems. The STOE is also intended to protect system availability to assure continuity of operations. Confidentiality beyond that required to protect the security subsystem itself or to protect against specific attacks on the ICS is not considered to be a large risk.

2.2 Scope of the STOE

The STOE consists of the security services and procedures, both automated and manual, which are designed to meet the security objectives defined to counter threats to the ICS.

The scope of the STOE is depicted graphically in Figure 2. Boxes with bold red borders depict the primary system security functions. These functions are: user authentication services (including user access control), physical access control, boundary protection, and data / device authentication. User authentication services control access to process control related computer systems including the human machine interface (HMI) and remote diagnostics and maintenance. In addition, user authentication is used by the physical access control system to authenticate personnel for physical access. Data / device authentication is shown as a separate function to emphasize the need for data and command signal authentication. Note that the corporate intranet is in the external environment of the STOE.

The blue lines from actuator to controlled process and from controlled process to sensor indicate that these are physical connections representing the direct interactions that take place. The rest of the diagram depicts logical connections. Security controls based on management and operating procedures are not shown in the Figure.

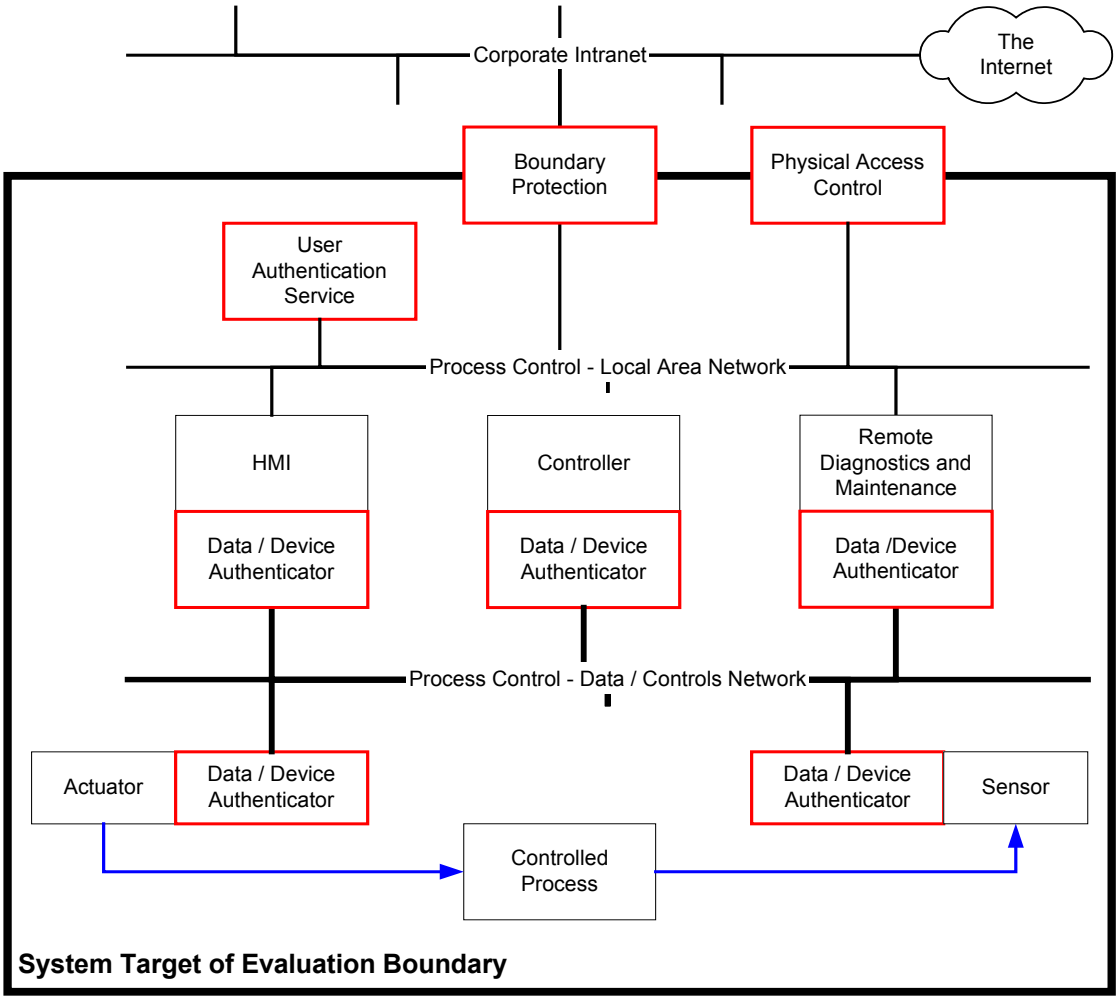

Figure 2 ***Graphical depiction of System Target of Evaluation***

The scope of the STOE includes the technical and non-technical elements identified in Table 1.

Table 1 –Scope of the STOE

STOE Components	Hardware/Software Components
Physical Boundary Protection	Access control
Logical Boundary Protection	Firewall
Data authentication	Authentication service, data / device authenticators
User Authentication	Authentication service, integration with physical access control

Continuity of Operations	System backup and recovery, Backup power
Operating procedures	Backup frequency, password requirements, etc.
Training	Security training, etc.
Management procedures	Staff selection criteria, disciplinary measures, etc.

2.3 Security Features

Editor's Note: The table below will be updated following confirmation of the security objectives by PCSRF members.

The STOE provides the following security features:

Table 2 – Summary of STOE Security Features

Feature	Description
Authentication	TBD
Integrity	TBD
Boundary Protection	TBD
Access control	TBD
Integration of access control with user authentication	TBD
Backup / Recovery	TBD
Non-interference with safety critical functions	TBD
Emergency power	Emergency power sufficient to allow for graceful shutdown of the ICS and the controlled process in the event that primary and secondary power fail.

2.4 Features Outside of Scope

Features outside the scope of the defined STOE and thus not evaluated are:

- General physical protection outside the scope of the STOE
- Enterprise intranet protection
- Protection of "business" information and systems other than that generated by the ICS while it resides within the ICS.
- Primary and secondary power
- General corporate security policies, procedures and training (the STOE will only address ICS specific policies, procedures and training)
- TBD

3 STOE Security Environment

In order to clarify the nature of the security problem that the STOE is intended to solve, this section describes the following:

- Any assumptions about the security aspects of the environment and/or of the manner in which the STOE is intended to be used.
- Any known or assumed threats to the assets against which specific protection within the STOE or its environment is required.
- Any organizational security policy statements or rules with which the STOE must comply.

3.1 Secure Usage Assumptions

The following assumptions relate to the operation of the TOE:

Table 3 – Secure Usage Assumptions

Name	Description
A.PHYSICAL_ACCESS	In accordance with organizational policy physical access controls are applied at designated physical access points throughout the system whose perimeters are defined by the organization, and personnel with authorized access is documented and maintained. Entry to secure areas is controlled and monitored on a periodic basis.
A.COMMS_ACCESS	In accordance with organizational policy, physical access to communication media, and connections to the media, and services allowed to go over the communications media (e.g., internet access, e-mail) is controlled, as is access to devices that display or output system control information.
A.EXTERNAL	The ICS network may have connectivity with non-ICS system networks through which Internet connectivity is possible.
A.REMOTE	Remote access to ICS components may be available to authorized individuals.

3.2 Threats to Security

Threats may be addressed either by the STOE or by its intended environment (for example, using personnel, physical, or administrative safeguards not provided by the STOE). These two classes of threats are discussed separately.

Threats are characterized in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. Threats agents are described as a combination of expertise, available resources, and

motivation. Attacks are described as a combination of attack methods, any vulnerabilities exploited, and opportunity.

3.2.1 Threats Addressed by the STOE

The following sections document the threat agents, attacks and assets relevant to the STOE. The last section combines all three aspects into a list of threats to be countered by the STOE.

3.2.1.1 Threat Agents

Threats agents are characterized through a combination of expertise, available resources, and motivation. The threat agents relevant to the STOE have been captured below in Table 4.

Table 4 – Threat Agents for the STOE

Threat Agent Label	Description[1]			
	Threat Agent	Expertise	Resources	Motivation
AGENT.INSIDER	Trusted employee, contractor, vendor or customer	Low/High	Substantial	Non-malicious
AGENT.EVIL_INSIDER	Trusted employee, contractor, vendor or customer acting inappropriately	Low/High	Substantial	Malicious
AGENT.PRIOR_INSIDER	Former trusted employee, contractor, vendor or customer	Low/High	Moderate	Malicious
AGENT.OUTSIDER	Unauthorized external party	High	Minimal/ Moderate	Malicious
AGENT.NATURE	Environmental sources of threats such as earthquakes, flood and fire	N/A	Substantial	N/A

Evil insiders include those legitimate users on the internal ICS network who misuse privileges or impersonate higher-privileged users.

[1] The descriptions for expertise, resources and motivation correspond to those defined for "capability of the attacker", "resources of the attacker", and "intent of the attacker" from Appendix E of NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems.

Outsiders include those intruders gaining access to the ICS from the Internet, dialup lines, physical break-ins, or from partner (supplier or customer) networks linked to the corporate network.

3.2.1.2 Attacks

Attacks are described as a combination of attack methods, any vulnerabilities exploited, and opportunity.

3.2.1.2.1 Sources of Vulnerability

The sources of vulnerability applicable to the STOE have been captured below. Please note that these sources of vulnerability should be further refined by the SST author to identify specific vulnerabilities applicable to the their own instantiation of the STOE.

Editor's note: The table below refers to sources or categories of vulnerabilities applicable to an ICS. It is envisaged that the categories of vulnerabilities listed below will be refined by the SST author as each STOE will have vulnerabilities specific to their own security environment in which the ICS is deployed.

Table 5 - Vulnerabilities of the STOE

Vulnerability Label	Vulnerability	Description
V.PLAINTEXT	Use of clear text protocols	The use of clear text protocols and the transmission of business and control data unencrypted over insecure communication channels (e.g. FTP, TELNET).
V.SERVICES	Unnecessary services enabled on system components	The presence of unnecessary system services on key ICS components and subsystems that may be exploited to negatively impact on system security (e.g. sendmail, finger services).
V.REMOTE	Remote access vulnerabilities	Uncontrolled external access to the corporate network (e.g. through the Internet) allowing unauthorized entry to the interconnected ICS network. Also includes vulnerabilities introduced through poor VPN configuration, exposed wireless access points, uncontrolled modem access (e.g. through networked faxes) and weak remote user authentication techniques.
V.ARCHITECTURE	Poor system architecture design leading to weaknesses in system security posture	Business and operational requirements impacting on the effectiveness of deployed or planned security measures to protect the confidentiality, integrity and availability of the ICS and its components. Poor security architecture may also lead to the bypass and tamper of ICS security functions.

Vulnerability Label	Vulnerability	Description
V.DEVELOPMENT	Poor system development practices leading to weakness in system implementation	Lack of quality processes (e.g. configuration management, quality testing) leading to errors in system implementation and third party products such as buffer overflows and errors in control algorithms.
V.NOPOLICIES	Inadequate system security policies, plans and procedures	Lack of formal system policies, plans and procedures (e.g. weak password policies, no incident response plans, irregular compliance audits, poor configuration management policies and procedures, poor system auditing practices, backup procedures etc).
V.SPOF	Single Points of Failure	Poor security architecture design leading to one or more single points of failure in the ICS and resulting in system unavailability.
V.NOTRAINING	Inadequate user training	Inadequate training on system security issues leading to poor user security awareness.
V.3RDPARTY	Unauthorized access to ICS via 3rd party network	Unauthorized user access to the ICS or its components via a 3rd party network connection.
V.NORISK	Lack of risk assessment	Inadequate risk assessment activities performed on critical assets leading to a poor understanding of the security posture of the ICS and the security controls needed to counter security risks to the organization.

3.2.1.2.2 Attack Descriptions

The generic types of attack relevant to the STOE have been captured below. Please note that the referenced vulnerabilities have been defined in the previous section.

Table 6 – Attack Methods against the STOE

Attack Label	Description			
	Attack	Method	Vulnerabilities	Opportunity[2]

[2] The description for opportunity relates to whether the attack can be conducted within the ICS network (locally) or outside the protected boundary of the ICS network (remotely).

Attack Label	Description			
	Attack	Method	Vulnerabilities	Opportunity[2]
ATTACK.SNIFF	Unauthorized traffic analysis	Packet capture tool, keystroke logger etc	V.PLAINTEXT, V.ARCHITECTURE, V.REMOTE, V.3RDPARTY, V.NORISK	Locally & Remotely
ATTACK.REPLAY	Unauthorized replay of captured traffic	Packet capture tool, keystroke logger etc	V.PLAINTEXT, V.ARCHITECTURE, V.REMOTE, V.3RDPARTY, V.NORISK	Locally & Remotely
ATTACK.SPOOF	Impersonating an authorized user	Exploitation of weak user authentication mechanism	V.PLAINTEXT, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.3RDPARTY, V.NORISK	Locally & Remotely
ATTACK.DOS	Overloading the network	Distributed denial of service attack from the Internet causing system downtime	V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.3RDPARTY, V.NORISK	Remotely
ATTACK.ERROR	Operator error	ICS system operator error causing security breach	V.SERVICES, V.NOPOLICIES, V.NOTRAINING, V.NORISK	Locally
ATTACK.SOCIAL	Social engineering of authorized users	Unsolicited contact with employee with the intent of discovering user credentials or acquiring sensitive information	V.NOPOLICIES, V.NOTRAINING, V.NORISK	Locally & Remotely
ATTACK.VIRUS	Virus infection of ICS system components	Virus propagation via email system or Internet downloaded content (e.g. Trojan)	V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY, V.NORISK	Locally

Attack Label	Description			
	Attack	Method	Vulnerabilities	Opportunity[2]
ATTACK.DESTROY	Destruction of ICS control data, business data or configuration information	File deletion on compromised ICS file servers	V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.NORISK	Locally & Remotely
ATTACK.MODIFY	Modification of ICS control data, business data or configuration information	File modification on compromised ICS file servers	V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.NORISK	Locally & Remotely
ATTACK.BYPASS	Bypass of system security functions and mechanisms	Modification of ICS configurations of components	V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.NORISK	Locally & Remotely
ATTACK.PHYSICAL	Compromise of poorly implemented and/or controlled physical security mechanisms	Unauthorized access to physically secured areas housing system assets (e.g. perimeter security breach)	V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING, V.NORISK	Locally
ATTACK.NATURE	Acts of nature causing system unavailability	Environmental occurrences such as earthquake, flood and fire	V.ARCHITECTURE, V.NOPOLICIES, V.NOTRAINING V.SPOF, V.NORISK	Locally

3.2.1.3 Assets

Assets protected by the STOE include the following:

Table 7 – Assets protected by the STOE

Asset Label	Asset	Description
ASSET.ACTUATOR	Actuator	One or more devices that receive the controlled variables from the controller and feeds them into the controlled process for action.

Asset Label	Asset	Description
ASSET.SENSOR	Sensor	One or more devices that sense or detect the value of a process variable and generates a signal related to the value (includes the sensing and transmitting parts of the device).
ASSET.CONTROLLER	Controller	The computer system or components that processes sensor input, executes control algorithms and computes actuator outputs (e.g. Programmable Logic Controllers).
ASSET.HMI	HMI	The hardware or software through which an operator interacts with a controller, providing a user with a view into the manufacturing process for monitoring or controlling the process.
ASSET.REMOTE	Remote Diagnostics & Maintenance	The hardware and software devices responsible for diagnostic and maintenance activities performed on the ICS from remote locations (e.g. Remote Terminal Units, pcAnywhere). May also include the communications mechanism or protocol used to access to the ICS (e.g. VPN).
ASSET.COMMS	Communications Infrastructure	The communications infrastructure (including equipment) used to bridge the control loop within an ICS. Also includes the network protocols used to integrate ICS components and subsystems (e.g. Ethernet, wireless, RS-232 etc).
ASSET.CTRLPROCESS	Controlled Process	The process subject to analysis and control by the ICS (including the inputs and outputs to the process).
ASSET.CTRLINFO	Process Control Information	The process control information being collected by, processed by, stored on and transmitted to or from the components that constitute the process control network
ASSET.BUSINFO	Process Control Business Information	The process control business or financial information being created by, processed by, stored on and transmitted to or from the components that constitute the process control network.

3.2.1.4 Threat Description

Using the description of the threat agents, attacks and assets captured in the previous sections, each of the threats relevant to the STOE have been characterized below:

Table 8 – Threats countered by the STOE

Threat Label	Threat	Description
T.DISCLOSURE	Unauthorized Information Disclosure	An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.SNIFF, ATTACK.SOCIAL) to acquire sensitive information (ASSET.COMMS, ASSET.CTRLINFO, ASSET.BUSINFO) stored on ICS components.
T.EVIL_ANALYSIS	Unauthorized Analysis	An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.SNIFF, ATTACK.SOCIAL) to analyze sensitive information flows (ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO) protected by the STOE.
T.EVIL_MODIFICATION	Unauthorized Modification	An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.MODIFY, ATTACK.BYPASS, ATTACK.SNIFF) to modify sensitive information (ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO) stored on ICS components.
T.EVIL_DESTRUCTION	Unauthorized Destruction	An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.DESTROY, ATTACK.BYPASS) to destroy sensitive information (ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO) stored on ICS components.
T.CTRL_TAMPER	Tampering with control components	The tampering of ICS components (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS) by malicious individuals (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) via the following attacks (ATTACK.MODIFY, ATTACK.BYPASS, ATTACK.PHYSICAL).
T.BAD_COMMAND	Integrity of Control Commands	An authorized operator (AGENT.INSIDER) accidentally issues bad commands (ATTACK.ERROR) resulting in the modification of controlled ICS processes and components (ASSET.CTRLPROCESS, ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI).
T.SPOOF	Spoofing legitimate users of the STOE	An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.SNIFF, ATTACK.SPOOF, ATTACK.SOCIAL) to obtain user credentials (ASSET.REMOTE, ASSET.COMMS) stored on ICS server components to impersonate authorized users.

Threat Label	Threat	Description
T.REPUDIATE	Identity repudiation	An authorized user (AGENT.INSIDER) denies having performed an action (ATTACK.ERROR) on the ICS interactive systems (ASSET.REMOTE, ASSET.COMMS, ASSET.HMI).
T.DOS	Denial of Service	An unauthorized individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.DESTROY, ATTACK.DOS) that denies service to valid users by making ICS components (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS) temporarily unavailable or unusable.
T.PRIVILEGE	Elevation of privilege	An unprivileged individual (AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.ERROR, ATTACK.SNIFF, ATTACK.SPOOF, ATTACK.SOCIAL) to obtain user credentials (ASSET.REMOTE, ASSET.COMMS) stored on ICS server components to elevate privileged access to ICS components for malicious purposes.
T.NO_FAULT_RECORD	Fault Detection	Faults generated by the system (AGENT.INSIDER) as a consequence of operator error and/or security breach (ATTACK.ERROR) while performing their routine tasks are not detected nor audited on ICS interactive systems (ASSET.REMOTE, ASSET.COMMS, ASSET.HMI) for further analysis and correction.
T.DISASTER	System Unavailability due to Natural Disaster	A natural disaster (AGENT.NATURE) ceases operation of one or more components of the ICS (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS) as a consequence of earthquake, fire, flood or other unpredictable event (ATTACK.NATURE).
T.OUTAGE	System Unavailability due to Power Outage	A natural disaster, malicious or non-malicious individual (AGENT.NATURE, AGENT.INSIDER, AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) inadvertently (or otherwise) causes a power outage affecting the availability of one or more components of the ICS (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS).
T.INFECTION	Virus Infection	An individual (AGENT.INSIDER, AGENT.EVIL_INSIDER, AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) maliciously or accidentally introduces a virus to the ICS network (ATTACK.VIRUS) causing unnecessary system downtime and corruption of data (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO).

Threat Label	Threat	Description
T.PHYSICAL_ACCESS	Unauthorized physical access	An unauthorized individual (AGENT.PRIOR_INSIDER, AGENT.OUTSIDER) directs an attack (ATTACK.PHYSICAL) to gain physical access to protected ICS components (ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS).

3.2.2 Threats Addressed by the Operating Environment

This SPP has not identified any threats relevant to the operating environment. Organizational security policy P.ENVIRONMENT assumes that adequate security controls have been deployed to address the threats relevant to the STOE operating environment.

3.3 Overarching Organizational Security Policies

This section describes the Overarching Organizational Security Policies (OOSPs) that define the broader context of the organization which support and govern the use of a system. These will form part of the basis for deriving the actual organizational security policies (OSPs) to be included as part of a specific STOE.

The scope of organizational security policy includes both the organizational security policies of the organization that has responsibility for operating the industrial control system as well as those for any external organizations that the industrial control system interacts with. Security related organizational policies include the following:

Table 9 – Organizational Security Policies

Name	Description
P.EVENT	The organization shall monitor security events to ensure compliance with security policies (e.g. security incident response plan).
P.PERSONNEL	The organization shall have in place policies, training programs, and reporting and enforcement mechanisms such that personnel know their security role in the organization.
P.INFRASTRUCTURE	The organization shall provide an organizational structure to establish the implementation of the security program, in which the policies can be established, maintained and enforced throughout the organization.
P.CONFIGURATION	The organization shall provide management and operational security controls necessary to manage the system's configuration during operations and evaluate and control changes to ensure that the system remains secure.

Name	Description
P.PHYSICAL	Adequate physical security shall be provided to detect or prevent unauthorized access or connection to the system and its components.
P.POLICY	The organization and system shall comply with organizational and regulatory policies and controls governing the use of, and implemented by the system to ensure secure operations.
P.ASSETS	The organization shall provide documentation of the system and its components, to understand the overall security posture.
P.SAFETY	The organization shall comply with relevant standards to ensure the safety of the system and its operators.
P.NO_INTERFERE	ICS security controls shall be implemented so as not to impede the minimum required operational capabilities of the ICS, and so as to not impede the safety systems that protect the ICS.
P.BUSINESS	The ICS shall be operated in accordance with a business continuity policy that addresses the identification of and response to events that adversely affect the ability of the ICS to operate in fulfilling its design goals (e.g. power outages, acts of nature etc).
P.RISK	The ICS shall be designed, implemented, and operated to meet the risk objectives resulting from a system life-cycle risk management program. The risk management program shall establish a comprehensive and integrated set of risk management goals for issues affecting ICS operation, safety and security.
P.ENVIRONMENT	The STOE operating environment shall have adequate security controls to counter those threats originating from outside of the defined STOE. The implementation and maintenance of these security controls should be in accordance with organizational security policies similar to those listed in this table and be selected based on the outcomes of a risk assessment.

4 Risks

The security risks are a further instantiation of the security problem. The element of risk is captured by the SPP to determine the relative importance of the security needs of the STOE and its operating environment. They guide the specification of the security objectives by ensuring that only those security needs seen as critical to the organization are addressed by the STOE or its operating environment.

Each risk is a product of asset value, assessed level of relevant threats, and associated vulnerabilities (as identified in the previous section). It represents the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organization.

Please note that this SPP has not specified the level of risk. Rather, it is intended that the SST author evaluate and prioritize the level of each risk according to their own ICS implementation (based on the combination of the value of each asset to the organization, the impact and probability rating of each threat successfully exploiting the identified vulnerabilities, and the effectiveness of existing security controls). Further guidance on the completion and relevance of this section can be found in chapter 7.

4.1 Risk Categories applicable to the STOE

The categories of security risks relevant to the STOE are described in Table 10. The table references the threats, vulnerabilities and assets identified in the previous chapter.

Editor's Note: At this level of abstraction the SPP has only captured the categories of risk applicable to the generic ICS described by this SPP. It is anticipated that future SPPs and SSTs will identify specific risks relevant to the author's own organizational context, and therefore expand upon the generic risks presented in this chapter.

Editor's Note: The next version will ensure consistency between the identified risk categories and the security environment and security objective chapters.

Table 10 – Identified Risk Categories for the STOE

Risk Category Label	Risk Category Description	Threats	Vulnerabilities	Assets
RISK.MANAGE	Risks associated with the security roles and responsibilities applicable to all ICS users, as well as risks associated with the successful implementation of the organizational security policies.	T.BAD_COMMAND, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD,	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS

Risk Category Label	Risk Category Description	Threats	Vulnerabilities	Assets
RISK.SECPOLICY	Risks associated with the development, endorsement and maintenance of the instruction stipulated by the corporate security policies.	T.BAD_COMMAND, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, T.INFECTION	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.RISKMAN	Risks associated with the management of the risk assessment processes for the ICS.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE , V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.COMPLY	Risks associated with not meeting internal and statutory requirements.	TBD	V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.ASSETCTRL	Risks associated with asset classification, labelling, media management and accountability.	T.REPUDIATE, T.PRIVILEGE, T.INFECTION, T.PHYSICAL_ACCESS	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO

Risk Category Label	Risk Category Description	Threats	Vulnerabilities	Assets
RISK.PERSONNEL	Risks associated with personnel vetting, security awareness, training, separation of duties and system usage agreements.	T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.PHYSICAL	Risks associated with unauthorized physical access and/or damage to system components.	T.PHYSICAL_ACCESS	V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS
RISK.ENVIRON	Risks associated with the effects of natural disasters, such as fire, flood and earthquake.	T.DISASTER	V.ARCHITECTURE V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.EVIL_ACCESS	Risks associated with the illicit use, modification and destruction of company data or inappropriate access to information. Risks associated with the inability to make individuals accountable for the actions they take when using the systems.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.NEED2KNOW	Risks associated with the threat to information confidentiality and privacy, unauthorised disclosure and clear desk practices.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.SPOOF, T.PRIVILEGE	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO

Risk Category Label	Risk Category Description	Threats	Vulnerabilities	Assets
RISK.INTEGRATE	Risks associated with the integration of security requirements into the systems development cycle and the selection of third party products.	TBD	V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.NETCOMMS	Risks associated with the protection of network communications at the logical and physical layers.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.NO_FAULT_RECORD, T.INFECTION, T.PHYSICAL_ACCESS	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.CONNECT	Risks associated with connections to other IT systems.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.INFECTION	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.INTERNET	Risks associated with the use of the Internet and email services both internal and external to the ICS.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.INFECTION	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.REMOTE	Risks associated with the connection of remote users to the ICS network.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.SPOOF, T.DOS, T.PRIVILEGE, T.INFECTION	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO

Risk Category Label	Risk Category Description	Threats	Vulnerabilities	Assets
RISK.ONLINE	Risks associated with the delivery of online services, including statutory requirements, security issues and controls, publishing and third-party security.	T.DISCLOSURE, T.DOS, T.NO_FAULT_RECORD, T.INFECTION	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.OPSMANAGE	Risks associated with managing system changes, such as changes not approved or audited correctly, lack of consultation with relevant parties, loss of skilled people, and lack of correct documentation. Risks associated with the use of technology for data and system control, including data protection, backup, disaster recovery, inadequate security, and insufficient capacity, etc.	T.DISCLOSURE, T.EVIL_ANALYSIS, T.EVIL_MODIFICATION, T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.SPOOF, T.REPUDIATE, T.DOS, T.PRIVILEGE, T.NO_FAULT_RECORD, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO
RISK.IDS	Risks associated with security auditing, security breach detection and response, incident reporting and forensic evidence requirements.	T.BAD_COMMAND, T.REPUDIATE, T.NO_FAULT_RECORD,	V.SERVICES, V.NOPOLICIES, V.NOTRAINING, V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS
RISK.CONTINUITY	Risks associated with ensuring the uninterrupted availability of all key business resources required to support essential (or critical) business activities.	T.EVIL_DESTRUCTION, T.CTRL_TAMPER, T.BAD_COMMAND, T.DOS, T.DISASTER, T.INFECTION, T.PHYSICAL_ACCESS	V.PLAINTEXT, V.SERVICES, V.REMOTE, V.ARCHITECTURE, V.SPOF, V.NOPOLICIES, V.NOTRAINING, V.3RDPARTY V.NORISK	ASSET.ACTUATOR, ASSET.SENSOR, ASSET.CONTROLLER, ASSET.HMI, ASSET.REMOTE, ASSET.COMMS, ASSET.CTRLPROCESS, ASSET.CTRLINFO, ASSET.BUSINFO

4.2 Risks to the External Operating Environment

This SPP has not identified any risks relevant to the external operating environment. Organizational security policy P.ENVIRONMENT assumes that adequate security controls have been deployed to mitigate the risks to the STOE external operating environment.

5 Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterized in the "Security Environment" section of the SPP, is to be addressed. Just as some threats are to be addressed by the STOE and others by its intended environment, some security objectives are for the STOE and others are for its environment. These two classes of security objectives are discussed separately.

5.1 Security Objectives for the STOE

The security objectives for the STOE are as described in the following table.

Table 11 – Security Objectives for the STOE

Objective Label	Objective Description
O.BOUNDARY_PROTECTION	The STOE must provide protection at the physical boundaries of the ICS to prevent access to the process control network by unauthorized users; and to prevent unauthorized access to the ICS and the physical plant.
O.RISK	ICS risk assessment shall be conducted throughout the life-cycle of an ICS, such that a documented and approved risk assessment process is conducted initially, and reviewed with each change to the manufacturing process or change to the ICS; and to ensure that changing vulnerabilities do not degrade the security of the ICS.
O.NON_INTERFERENCE	The ICS security functions shall be implemented in a non-interfering manner such behavior of the ICS functions and safety functions are able to meet their performance constraints.
O.DATA_BACKUP	The STOE must include provisions for ICS data and control information (including executable software and control data) to assure the ability for timely recovery to an operating state if the ICS is compromised or damaged. The data backup procedures should follow industry best practices including (but not limited to) secondary storage locations, testing of recovery procedures, and a back up interval either driven by configuration changes or a specified time interval or a combination of both.
O.DATA_AUTHENTICATION	The STOE shall authenticate configuration change commands such that configuration (control algorithms, set points, limit points, etc.) cannot be changed unless the integrity of the command can be positively established. The STOE shall authenticate financial or other business critical information sent from the STOE to external systems with a minimum of a time stamped digital signature.

Objective Label	Objective Description
O.BACKUP_POWER	Emergency backup power will be available to the ICS with sufficient capacity to permit safe and recoverable shutdown of the process if external power is lost.
O.CONTINUITY	The ICS shall ensure continuity of operations in accordance with a business continuity policy that addresses a known set of anticipated events that might adversely affect the operational capability of the ICS.
O.VERIFY	The ICS components as an integrated system shall be capable of undergoing verification analysis and testing to ensure that the ICS: • Meets is security design specification; • Is properly installed and integrated; • Is properly configured.
O.OWNERSHIP	Identified roles and responsibilities, together with explicit authority to ensure operational security within the management infrastructure; an organization wide, security infrastructure.
O.MIGRATION	The ICS shall have a migration strategy providing the capability to govern the evolution of the control system throughout its security operational life cycle. The migration strategy shall address at a minimum: • Assessment of new vulnerabilities and appropriate/necessary mitigating actions to control/reduce new vulnerabilities. This may include maintenance of the current system state (components, configuration, patches, etc). • The integration between computer implemented and personnel implemented procedures.
O.COMPLIANCE	The ICS shall be operated in compliance with relevant governing mandates.
O.COLLABORATE	Policies governing the roles, responsibilities and activities authorized for individuals not employed by the control system operating organization shall be developed. The policies shall establish methods for on-site internal, on-site remote, and off-site remote access to control system resources

Objective Label	Objective Description
O.ACCESS_CONTROL	The ICS shall provide the capability to grant or deny access to control system resources based upon the action being performed, and the authorizations associated with authorized subjects. The ICS shall deny unauthorized agents access to every control system resource. The ICS shall require that each agent authorized to use the control system is identified and is provided with credentials to authenticate their identity. The ICS must be able to include knowledge of the control system state and/or the controlled process state when making an access control decision. The ICS shall include knowledge of time and location in the rules for making an access control decision.
O.COMMS_INTEGRITY	The ICS shall provide the capability to prevent or detect, as required, the loss of integrity of the ICS operational communications capability. The ICS shall provide the capability to allow information flows only between authenticated and authorized endpoints. The ICS shall provide the capability to protect information flows from replay, substitution or modification. The ICS shall provide the capability to allow the recipient of an authorized information flow to verify the correctness of the received information.
O.AVAILABLE	The ICS shall have continuity of availability of operational capability. The ICS shall be capable of continuing operation if a control server is unavailable for any reason. The ICS shall be capable of continuing operation if the primary communications channel is unavailable for any reason.

Objective Label	Objective Description
O.CONTROL_INTEGRITY	The ICS shall provide the capability to prevent or detect, as required, the loss of integrity of the ICS operational system configuration and capability. The ICS shall provide the capability to restrict access to the functions used to establish and maintain the secure operational configuration of the ICS. The ICS shall be capable of performing self-tests to verify the configuration and integrity of the security functions of the ICS. The ICS shall provide the capability for self-test to be executed on startup, at periodic intervals, and on demand. The ICS shall be capable of responding to integrity failures.

5.2 Security Objectives for the External Operating Environment

This SPP has not identified any security objectives relevant to the external operating environment. Organizational security policy P.ENVIRONMENT assumes that adequate security controls have been deployed to address the security needs outside the scope of the STOE.

6 IT Security Requirements

6.1 STOE Security Functional Requirements

This section contains the functional requirements for the STOE. This includes system security functional requirements and system security assurance requirements. The requirements are primarily stated as logical requirements and cover information technology related requirements, requirements for system security policies and system security related operating procedures, and integration requirements addressing interfaces and interoperability between security system components. The functional requirements are listed in summary form in the table below.

Editor's Note: Table 12 and the text below it outline extensions to the functional requirements that is building on ISO system work in concert with NIST work building on security controls.

Table 12 – STOE Security Functional Requirements

No.	Component	Component Name
Class FAU: Audit		
1	FAU_ARP.1	Security alarms
2	FAU_GEN.1	Audit data generation
3	FAU_GEN.2	User identity association
4	FAU_SAA.1	Potential violation analysis
5	FAU_SAA.2	Profile based anomaly detection
6	FAU_SAA.3	Simple attack heuristics
7	FAU_SAA.4	Complex attack heuristics
8	FAU_SEL.1	Selective audit
Class FCS: Cryptographic support		
9	FCS_CKM.4	Cryptographic key management
10	FCS_COP.1	Cryptographic operation
Class FDP: User data protection		
11	FDP_ACC.1	Subset access control
12	FDP_ACC.2	Complete access control
13	FDP_ACF.1	Security attribute based access control
14	FDP_DAU.2	Data authentication

15	FDP_IFC.1	Subset information flow control
16	FDP_IFC.2	Complete information flow control
17	FDP_IFF.1	Simple security attributes
18	FDP_RIP.2	Full residual information protection
19	FDP_UCT.1	Basic data exchange confidentiality
20	FDP_UIT.1	Data exchange integrity
21	FDP_UIT.2	Source data exchange recovery
Class FIA: Identification & Authentication		
22	FIA_AFL.1	Authentication failure handling
23	FIA_ATD.1	User attribute definition
24	FIA_SOS.1	Verification of passwords
25	FIA_SOS.2	TSF generation of passwords
26	FIA_UAU.1	Timing of authentication
27	FIA_UAU.2	User authentication before any action
28	FIA_UAU.3	Unforgeable authentication
29	FIA_UAU.4	Single use authentication mechanisms
30	FIA_UAU.7	Protected authentication feedback
31	FIA_UID.1	Timing of identification
32	FIA_UID.2	User identification before any action
Class FMT: Management of functions in TSF		
33	FMT_MOF.1	Management of security functions behavior
34	FMT_MOF.2	Security function and security policy mapping
35	FMT_MSA.1	Management of security attributes
36	FMT_MTD.1	Management of TSF data
37	FMT_MTD.4`	Management of TSF data to policy mapping
38	FMT_REV.1	Revocation
39	FMT_SAE.1	Time limited authorization
40	FMT_SMF.1	Security management functions
41	FMT_SMR.1	Security roles
42	FMT_SMR.2	Restrictions on security roles
43	FMT_SMR.4	Security role to policy mapping

Class FEM: Security event monitoring		
44	FEM_EDI.1	Event definition and identification
45	FEM_EDI.2	Interaction of system event monitoring components
46	FEM_EDI.3	Alarm audit requirements
47	FEM_EDI.4	Alarm response
Class FPT: Protection of the TSF		
48	FPT_AMT.1	Abstract machine testing
49	FPT_FLS.1	Failure with preservation of secure state
50	FPT_ITA.1	Inter-TSF availability within a defined availability metric
51	FPT_ITC.1	Inter-TSF confidentiality during transmission
52	FPT_ITI.1	Inter-TSF detection of modification
31	FPT_ITI.2	Inter-TSF detection and correction of modification
52	FPT_PHP.1	Passive detection of physical attack
53	FPT_PHP.2	Notification of physical attack
54	FPT_PHP.3	Resistance to physical attack
55	FPT_PHP.4	Domain definition and alarm response
56	FPT_RCV.2	Automated recovery
57	FPT_RCV.3	Automated recovery without undue loss
58	FPT_RCV.4	Function recovery
59	FPT_RPL.1	Replay detection
60	FPT_SSP.1	Simple trusted acknowledgement
61	FPT_SSP.2	Mutual trusted acknowledgement
62	FPT_STM.1	Reliable time stamps
63	FPT_TDC.1	Inter-TSF data consistency
64	FPT_TRC.1	Internal TSF consistency
65	FPT_TST.1	TSF testing
Class FCM: Protection of System Configuration		
66	FCM_IDI.1	Identification information
67	FCM_IDI.2	Change requests and actions
68	FCM_IDI.3	Authorizations
Class FRU: Resource utilization		

70	FRU_FLT.1	Degraded fault tolerance
71	FRU_PRS.1	Limited priority of service
72	FRU_PRS.2	Full priority of service
Class FTP: Trusted path/channels		
73	FTP_ITC.1	Inter-TSF trusted channel
74`	FTP_ITP.1	Trusted path

The following sections contain the functional components from the Common Criteria Part 2 [CC2] (CC) with the operations completed. The standard CC text is in regular font; the text inserted by the System Protection Profile (SPP) author is in accordance with the conventions described in at the beginning of this document.

Editor's note: The security functional requirements listed in the above table will be specified in the next release of this document. Reviewers should ensure that high-level functionality (as captured by the security objectives) is consistent with their understanding of the STOE.

6.1.1 Logon Controls:

FIA_UID.1 Timing of identification
Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: **FIA_UID.1 Timing of identification**

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing **any other TSF-mediated actions** on behalf of that user.
Dependencies: **FIA_UID.1 Timing of identification**

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
Dependencies: **FIA_UAU.1 Timing of authentication**

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*].
Dependencies: No dependencies

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *attributes*].
Dependencies: No dependencies

6.1.2 Password Selection

FIA_SOS.1 Verification of *passwords*

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that *passwords* meet [assignment: *a defined quality metric*].

Dependencies: No dependencies

FIA_SOS.2 TSF Generation of *passwords*
Hierarchical to: No other components.
FIA_SOS.2.1 The TSF shall provide a mechanism to generate *passwords* that meet [assignment: *a defined quality metric*].
FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated *passwords* for [assignment: *list of TSF functions*].
Dependencies: No dependencies

FMT_SAE.1 Time-limited authorisation
Hierarchical to: No other components.
FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorized identified roles*].
FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.
Dependencies: **FMT_SMR.1 Security roles**
FPT_STM.1 Reliable time stamps

6.1.3 Authentication Data Protection

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.
Dependencies: **FIA_UAU.1 Timing of authentication**
(For passwords)

FMT_MTD.1Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FPT_RPL.1 Replay detection
Hierarchical to: No other components.
FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: *list of identified entities*].

FPT_RPL.1.2 The TSF shall perform [assignment: *list of specific actions*] when replay is detected.
Dependencies: No dependencies

6.1.4 Replay / Reuse

FIA_UAU.3 Unforgeable authentication
Hierarchical to: No other components.
FIA_UAU.3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2 The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.
Dependencies: No dependencies
FIA_UAU.4 Single-use authentication mechanisms
Hierarchical to: No other components.
FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(*s)].
Dependencies: No dependencies
---These are targeted to preventing replay attacks from captured control signals---

6.1.5 Session Suspension

FTA_SSL.1 TSF-initiated session locking
Hierarchical to: No other components.
FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.
FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].
Dependencies: **FIA_UAU.1 Timing of authentication**
FTA_SSL.2 User-initiated locking
Hierarchical to: No other components.
FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session,
by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].
Dependencies: **FIA_UAU.1 Timing of authentication**
FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].
Dependencies: No dependencies

6.1.6 User Accounts and Profiles

FMT_MTD.1Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

(User accounts and User profiles)

FIA_ATD.1 User attribute definition
Hierarchical to: No other components.
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].
Dependencies: No dependencies

(Definition of user security attributes contained in a user profile)

6.1.7 Role based access control

FDP_ACC.1 Subset access control
Hierarchical to: No other components.
FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].
Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.2 Complete access control
Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] **and all operations among subjects and objects covered by the SFP.**
FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].
FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].
FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].
Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialization

FMT_SMR.1 Security roles

Hierarchical to: No other components.
FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorized identified roles*].
FMT_SMR.1.2 The TSF shall be able to associate users with roles.
Dependencies: **FIA_UID.1 Timing of identification**

FMT_SMR.2 Restrictions on security roles

Hierarchical to: **FMT_SMR.1**
FMT_SMR.2.1 The TSF shall maintain the roles: [assignment: *the authorized identified roles*].
FMT_SMR.2.2 The TSF shall be able to associate users with roles.
FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: *a single user account is not assigned the two different roles associated with a two-man rule*] are satisfied.
Dependencies: **FIA_UID.1 Timing of identification**

Application Note: FDP_ACF.1 may be used to specify that particular operations require two distinct roles to authorize the action. FMT_SMR.2.3 can ensure that a user account

cannot be assigned to both roles (as used above). If there is more than one situation requiring implementation of a two-man rule the combination should be iterated for each set of roles.

6.1.8 Controls on RBAC Attributes

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].
Dependencies: **[FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles**

6.1.9 Firewall access control

FDP_IFC.1 Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].
Dependencies: **FDP_IFF.1 Simple security attributes**
FDP_IFC.2 Complete information flow control
Hierarchical to: FDP_IFC.1
FDP_IFC.2.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects* and *information*] and **all operations that cause that information to flow to and from subjects covered by the SFP.**
FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.
Dependencies: **FDP_IFF.1 Simple security attributes**

FDP_IFF.1 Simple security attributes
Hierarchical to: No other components.
FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].
FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].
FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].
FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorize information flows*].
FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].
Dependencies: **FDP_IFC.1 Subset information flow control**
FMT_MSA.3 Static attribute initialization

6.1.10 Audit events

FAU_GEN.1 Audit data generation
Hierarchical to: No other components.
FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [selection: *minimum, basic, detailed, not specified*] level of audit; and
c) [assignment: *other specifically defined auditable events*].
FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]
Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.2 User identity association
Hierarchical to: No other components.
FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.
Dependencies: **FAU_GEN.1 Audit data generation**
FIA_UID.1 Timing of identification

FMT_MTD.1Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].
Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FAU_SEL.1 Selective audit
Hierarchical to: No other components.
FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [selection: *object identity, user identity, subject identity, host identity, event type*]
b) [assignment: *list of additional attributes that audit selectivity is based upon*].
Dependencies: **FAU_GEN.1 Audit data generation**
FMT_MTD.1 Management of TSF data

6.1.11 Intrusion detection and response

FAU_ARP.1 Security alarms
Hierarchical to: No other components.
FAU_ARP.1.1 The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.
Dependencies: **FAU_SAA.1 Potential violation analysis**

FAU_SAA.1 Potential violation analysis
Hierarchical to: No other components.
FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.
FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;
b) [assignment: *any other rules*].
Dependencies: **FAU_GEN.1 Audit data generation**

FAU_SAA.2 Profile based anomaly detection
Hierarchical to: FAU_SAA.1
FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *the profile target group*].

FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.
FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].
Dependencies: **FIA_UID.1 Timing of identification**

FAU_SAA.3 Simple attack heuristics

Hierarchical to: FAU_SAA.1
FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the TSP.
FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].
FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.
Dependencies: No dependencies

FAU_SAA.4 Complex attack heuristics

Hierarchical to: FAU_SAA.3
FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the **following event sequences of known intrusion scenarios [assignment: *list of sequences of system events whose occurrence are representative of known penetration scenarios*] and** the following signature events [assignment: *a subset of system events*] that may indicate a potential violation of the TSP.

FAU_SAA.4.2 The TSF shall be able to compare the signature events **and event sequences** against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].
FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when **system activity** is found to match a signature event **or event sequence** that indicates a potential violation of the TSP.
Dependencies: No dependencies

6.1.12 Audit trail protection

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.
FAU_STG.1.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.
Dependencies: **FAU_GEN.1 Audit data generation**

FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1
FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.
FAU_STG.2.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.
FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion, failure, attack*].
Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.
FAU_STG.3.1 The TSF shall take [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].
Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3
FAU_STG.4.1 The TSF shall [selection: '*ignore auditable events*', '*prevent auditable events, except those taken by the authorized user with special rights*', '*overwrite the oldest stored audit records*'] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.
Dependencies: FAU_STG.1 Protected audit trail storage

6.1.13 Audit trail analysis / review

FAU_SAR.1 Audit review

120 This component will provide authorized users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.
Hierarchical to: No other components.
FAU_SAR.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: **FAU_GEN.1 Audit data generation**

FAU_SAR.2 Restricted audit review
Hierarchical to: No other components.
FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
Dependencies: **FAU_SAR.1 Audit review**

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components.
FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment: *criteria with logical relations*].
Dependencies: **FAU_SAR.1 Audit review**

6.1.14 TOE Integrity

FPT_PHP.1 Passive detection of physical attack
Hierarchical to: No other components.
FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
Dependencies: **FMT_MOF.1 Management of security functions behavior**

FPT_PHP.2 Notification of physical attack
Hierarchical to: FPT_PHP.1
FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.
FPT_PHP.2.3 For [assignment: *list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [assignment: *a designated user or role*] when physical tampering with the TSF's devices or TSF's elements has occurred.
Dependencies: FMT_MOF.1 Management of security functions behavior

FPT_PHP.3 Resistance to physical attack
Hierarchical to: No other components.
FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.
Dependencies: No dependencies

6.1.15 Data Authentication

FDP_DAU.2 Data authentication with identity of guarantor
Hierarchical to: **FDP_DAU.1**
FDP_DAU.2.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*].
FDP_DAU.2.2 The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information **and the identity of the user that generated the evidence.**
Dependencies: **FIA_UID.1 Timing of identification**

6.1.16 Data exchange integrity

FDP_UIT.1 Data exchange integrity
Hierarchical to: No other components.
FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.
Dependencies: **[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]**

6.1.17 Functions required to support dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.
Dependencies: No dependencies

FDP_ACF.1 Security attribute based access control
Hierarchical to: No other components.
FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].
Dependencies: **FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization**

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorized identified roles*].
Dependencies: **[FDP_ACC.1 Subset access control or**
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components.
FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the *SFP*.
FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorized identified roles*] to specify alternative initial values to override the default values when an object or information is created.
Dependencies: **FMT_MSA.1 Management of security attributes**
FMT_SMR.1 Security roles

FDP_IFC.1 Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].
Dependencies: **FDP_IFF.1 Simple security attributes**

FMT_MOF.1Management of security functions behavior
Hierarchical to: No other components.
FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behavior of, disable, enable, modify the behavior of*] the functions [assignment: *list of functions*] to [assignment: *the authorized identified roles*].
Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

6.1.18 Secure Communications Channels

FPT_ITA.1 Inter-TSF availability within a defined availability metric
Hierarchical to: No other components.
FPT_ITA.1.1 The TSF shall ensure the availability of [assignment: *list types of TSF data*] provided to a remote trusted product within [assignment: *a defined availability metric*] given the following conditions [assignment: *conditions to ensure availability*].
Dependencies: No dependencies

FPT_ITC.1 Inter-TSF confidentiality during transition

Hierarchical to: No other components.

The TSF shall protect all data transmitted from the TSF to a remote trusted product from unauthorized disclosure during transmission.

Dependencies: No dependencies

FPT_ITI.1 Inter-TSF detection of modification

Hierarchical to: No other components.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted product within the following metric: [assignment: *a defined modification metric*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted product and perform [assignment: *action to be taken*] if modifications are detected.

Dependencies: No dependencies.

FPT_ITI.2 Inter-TSF detection and correction of modification

Hierarchical to: FPT_ITI.1

FPT_ITI.2.3 The TSF shall provide the capability to correct [assignment: *type of modification*] of all TSF data transmitted between the TSF and a remote trusted product.

Dependencies: No dependencies.

FPT_SSP.1 Simple trusted acknowledgement

Hierarchical to: No other components.

FPT_SSP.1.1 The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission.

Dependencies: **FPT_ITT.1 Basic internal TSF data transfer protection**

FTP_SSP.2 Mutual trusted acknowledgement

Hierarchical to: FPT_SSP.1

FTP_SSP.2.2 The TSF shall ensure that the relevant parts of the TSF know the correct status of transmitted data among its different parts, using acknowledgements.

Dependencies: FPT_ITT.1 Basic internal data transfer protection.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

The TSF shall be able to provide reliable time stamps for the systems use.

Dependencies: No dependencies.

FPT_TDC.1 Inter-TSF basic data consistency

Hierarchical to: No other components.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted product.
FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.
Dependencies: No dependencies.

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, the remote trusted product*] to initiate communication via the trusted channel.
FPT_ITC.1.3 The TSF shall initiate communication via trusted channel for [assignment: *list of functions for which a trusted channel is required*].
Dependencies: No dependencies.

FTP_TRP.1 Trusted path
Hierarchical to: No other components.
FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communications paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FPT_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communications via the trusted path.
FPTTRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication,* [assignment: *other services for which trusted path is required*]].
Dependencies: No dependencies.

FDP_ETC.1 Export of user data without security attributes
Hierarchical to: No other components.
FDP_EDP.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside the TSC.
FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

6.1.19 Management Functions

FMT_MOF.2 Security policy and security function mapping
Hierarchical to: No other components.

FMT_MOF.2.1 The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].
Dependencies: **No Dependencies**

<Editor Note: The remaining management functions are extensions to ISO 15408, that is, they are not found in the ISO standard>

FMT_REV.1 Access revocation
Physical and IT access shall be revoked within [assignment: *time span*] for personnel whose employment or contractual relationship is terminated or for personnel who are temporarily not actively involved in process control and operations (for example, workers on strike, workers on a leave of absence, etc.)

FPT_PHP.5 Backup and Restore
The TSF shall include the capability to backup and restore the system configuration including critical programs, controller instructions and parameters, and instructions and parameters for all sensors and actuators. Backups shall be performed [assignment: frequency] and whenever critical operating parameters [assignment: identify the critical operating parameters] are changed.

FPT_PHP.5 Backup and Restore Self-Testing
The TSF backup and restore procedure shall be able to be self-tested during regular operations and planned maintenance. Self-Test to be evoked as part of FPT_TST.1.

6.1.20 Physical Security Requirements

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >

PHY_SOB.2 Strength of Boundary Access Control
The TSF shall provide physical access control to critical ICS components including, but not limited to: control room(s), servers, controller, sensors, actuators, and the physical plant under control. <Editor Note: This requirement is included as an example. Physical security requirements should be inserted in this section as appropriate to the specific nature of the target ICS. >

6.1.21 Security Event Monitoring

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >

FEM_EDI.1 Event Definition and Identification provides that an automated security event monitoring system be used to monitor, manage, and report pre-defined security events, which includes the type of event to be monitored, to include: security event identification, name of interface or component to be monitored, its physical location within the system, component name and function, any governing policies, and flow control of alarm reporting. Event definition specifies the system security event alarm parameter settings, and values for each pre-defined security event. It additionally identifies the System interface and component that monitors and reports the events, the system component that receives the event from the interface, processes it, and transmits the alarm; the location that alarm is to be reported, and the relationship of the event alarm to the system TSF.

FEM_EDI.2 Interaction of system event monitoring components defines the iinteractions of technical and operational and management security controls components that support event monitoring associated with the system environment. Also defines the system environment security controls event monitoring reporting mechanism from either direct or indirect interface with the System technical security controls components that support event monitoring. May be used in conjunction with FPT_PHP.

FEM_EDI.3 Alarm audit requirements define the audit requirements for the defined alarms.

FEM_EDI.4 Alarm response identifies that the alarm response to authorized pre-defined security event monitoring alarms be obtained and documented; identifies the roles and responsibilities that are defined for receipt of alarm and required action, including any timing constraints (possible roles are specified in FMT_SMR.1); defines security event alarm reporting procedures and mechanisms for the exchange of security event alarm information between the System IT and System environment security controls; and specifies that event alarm audit data be transformed to a specific format to support real-time analysis, and into a different useful format for delivery to authorised users for review (see application notes for FAU_SAA)

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
The TSF shall be able to provide reliable time stamps for the systems use.
Dependencies: No dependencies.

6.1.22 Requirements for interfaces between system components

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >

FPT_PHP.2 Authentication Integration
The TSF shall integrate authentication of user access with authentication for physical access such that user access is not granted for a user not identified by the physical access control as being physically present and such that user access is locked when the physical access control indicates that the user is no longer physically present.

6.1.23 Requirements for composability and interoperability between system components

FPT_PHP.4 Domain Definition and Response to Alarm
The TSF shall identify and define the domains, which comprise the system, the physical boundary for each domain, and the security policy(s), which governs each of the domains. The system security alarms may be tailored for the components being governed by the specific domain. The definition for each alarm shall be well defined, to include the alarm threshold, where it is reported, and the requisite system response.

This section documents any requirements specific to security composability that have not

6.1.24 Configuration requirements

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >

FCM_IDI.1 Configuration Change Requests and Actions
The STOE shall be subject to configuration management with an explicit change control and review process.

6.2 STOE Security Assurance Requirements

This section contains the assurance requirements for the TOE. The assurance requirements are listed in summary form in Table 13 below, with more detail on the assurance requirements following the Table. The general intent of the assurance requirements and associated system evaluation activities is to confirm that the acceptable level of residual risk as documented in the SPP is achieved in the operational system

The baseline evaluation assurance level (EAL) for Industrial Control Systems is EAL 3+. The "+" indicates that the EAL is as defined in ISO 15408 Part 3 with additional assurance requirements. In this case the additional requirements reflect the assurances associated with design, development, integration, testing and deployment of a system as opposed to a component or product. In addition, because the ICS is a system, a

combination of technical and operations and management security control elements must be considered.

Editor Note: Table 13 and the text below it outline extensions to the assurance requirements that is building on ISO system work in concert with NIST work on security controls.

Table 13 – STOE Security Assurance Requirements

No.	Component	Component Name
Class ACM: Configuration management		
1	ACM_CAP.3	Authorization controls
2	ACM_SCP.1	TOE CM Coverage
3	ACM_OBM.1	CM Operational Baseline and Maintenance
Class ADO: Delivery and Operation		
4	ADO_DEL.1	Delivery procedures
5	ADO_IGS.1	Installation, generation and start-up
6	ADO_SIC.1	Site interoperability check
Class AGD: Guidance documents		
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	AGD_OCD.1	System operational configuration definition guidance
Class ALC	**Life cycle support**	
10	ALC_DVS.1	Identification of security measures
11	ALC_FLR.3	Systematic flaw remediation
12	ALC_OPS.1	Operational security
Class ASA	**Security awareness**	
13	ASA_PPG.2	Verified operational security guidance
Class ASC	**O&M security**	
14	ASC_PPO.1	Verified policy and procedures
15	ASC_PFA.1	Asset records confirmation
16	ASC_OIN.1	Operational integration
Class ASD	**System Architecture**	
17	ASD_SAD.1	Operational system architecture design
18	ASD_IFS.1	Operational system interface functional specification

19	ASD_SSD.2	Subsystem design
20	ASD_IMP.1	Implementation representation
21	ASD_COM.1	System security concept of operations
Class ATE: Tests		
22	ATE_COV.2	Analysis of coverage
23	ATE_FUN.1	Functional testing
24	ATE_IND.2	Independent testing- sample
25	ATE_AST.3	Operational testing policy conformance
Class AVA: Vulnerability Assessment		
26	AVA_SOF.1	Strength of STOE security function evaluation
27	AVA_MSU.1	Examination of guidance
28	AVA_VLA.1	Developer vulnerability analysis
Class AMA: Assurance Maintenance		
29	ASA_AMP.1	Assurance maintenance plan
30	AMA_EVD.1	Evidence of assurance maintenance
31	AMA_SIA	Security impact analysis

6.2.1 Configuration Management (ACM)

Authorization Controls (ACM_CAP.3)

Dependencies: ALC_DVS.1 Identification of security measures

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

ACM_CAP.3.1C The reference for the STOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The STOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list **and a plan**.

ACM_CAP.3.4C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7C	**The CM Plan shall describe how the CM system is used.**
ACM_CAP.3.8C	**The evidence shall demonstrate that the CM system is operating in accordance with the CM Plan.**
ACM_CAP.3.9C	**The CM documentation shall provide evidence that all configuration have been and are being effectively maintained under the CM system.**
ACM_CAP.3.10C	**The CM system shall provide measures such that only authorized changes are made to the configuration items.**
ACM_CAP.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

STOE CM Coverage (ACM_SCP.1)

Dependencies: ACC_CAP.3 Authorization controls

ACM_SCP.1.1D	**The developer shall provide a list of configuration items for the TOE.**
ACM_SCP.1.1C	**The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.**
ACM_SCP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Operational Baseline & Maintenance (ACM_OBM.1)

Dependencies: ACM_CAP.3 Authorization controls
ACM_SCP.1 TOE CM coverage

ACM_OBM.1.1D	**The developer/system owner shall use a CM system for the initial/most recent evaluated system, which shall be called the "Baseline".**
ACM_OBM.1.2D	**The CM system shall track and monitor each change, proposed and actual to the system Baseline, and its evaluation status.**
ACM_OBM.1.3D	**The CM system shall report the current operational system configuration baseline.**
ACM_OBM.1.4D	**The developer/system owner shall provide CM documentation of the Baseline system.**
ACM_OBM.1.1C	**The CM System shall uniquely identify the System TOE Baseline, each associated change, and its evaluation status.**
ACM_OBM.1.2.C	**The CM Plan shall describe how the system baseline is maintained, and changes to the baseline are tracked and controlled.**
ACM_OBM.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2 Delivery and Operation (ADO)

Delivery Procedures (ADO_DEL.1)

Dependencies: No dependencies.

ADO_DEL.1.1D	**The developer shall document procedures for delivery of the System TOE or parts of it to the user.**
ADO_DEL.1.2D	**The developer shall use the delivery procedures**.
ADO_DEL.1.1C	**The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the System TOE to a user's site**.
ADO_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Installation, Generation and Start-up Procedures (ADO_IGS.1)

Dependencies:	No dependencies.
ADO_IGS.1.1D	**The developer shall document procedures necessary for the secure installation, generation, and start-up of the System TOE.**
ADO_IGS.1.1C	**The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the System TOE**.
ADO_IGS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E	The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Site Interoperability Check (ADO_SIC.1)

Dependencies:	No dependencies.
ADO_SIC.1.1D	**The developer shall document procedures necessary to ensure that components and interfaces that comprise the System TOE, especially those to legacy security controls and interfaces can be started up and interoperate in a secure manner.**
ADO_SIC.1.1C	**The site interoperability check procedures documentation shall describe the steps necessary for verification of secure start-up and interoperation of the System TOE in its environment**.
ADO_SIC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_SIC.1.2E	The evaluator shall determine that the start-up and interoperability check procedures result in a secure configuration.

6.2.3 Guidance Documents (AGD)

Administrator Guidance (AGD_ADM.1)

Dependencies:	ASD_SAD.1 Operational System Architecture Design

AGD_ADM.1.1D	**The developer shall provide administrator guidance addressed to system administrative personnel.**
AGD_ADM.1.1C	**The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the System TOE.**
AGD_ADM.1.2C	**The administrator guidance shall describe how to administer the System TOE in a secure manner.**
AGC_ADM.1.3C	**The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.**
AGC_ADM.1.4C	**The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.**
AGC_ADM.1.5C	**The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values, as appropriate.**
AGC_ADM.1.6C	**The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.**
AGC_ADM.1.7C	**The administrator guidance shall be consistent with all other documentation supplied for evaluation.**
AGC_ADM.1.8C	**The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.**
AGD_ADM.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

User Guidance (AGD_USR.1)

Dependencies: ASD_SAD.1 Operational System Architecture Design

AGD_USR.1.1D	**The developer shall provide user guidance.**
AGD_USR.1.1C	**The user guidance shall describe the functions and interfaces available to the non-administrative users of the System TOE**

available to the non-administrator users of the System TOE.

AGD_USR.1.2C **The user guidance shall describe the use of user-accessible security functions provided by the System TOE.**

AGD_USR.1.3C **The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.**

AGD_USR.1.4C **The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of the TOE security environment.**

AGD_USR.1.5C **The user guidance shall be consistent with all other documentation supplied for evaluation.**

AGD_USR.1.6C **The user guidance shall describe all security requirements for the IT environment that are relevant to the user.**

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

System Operational Configuration Definition Guidance (AGD_OCD.1)

Dependencies: ASD_SAD.1 Operational System Architecture Design

ASD_COM.1 Operational System Security Concept of Operations

AGD_OCD.1.1D **The developer/integrator/system owner shall provide configuration guidance that defines the security relevant configuration parameters that support the integration of the system components and that allow the system security functions to implement and enforce the system security concept of operations and associated policies.**

AGD_OCD.1.1C **The configuration guidance shall describe the security configuration parameters available to the system integrator or equivalent users/administrator of the System TOE with that role and responsibility.**

AGD_OCD.1.2C **The configuration guidance shall describe the use of security parameters configurable by the TOE to implement and enforce the system security policies.**

AGD_OCD.1.3C	**The configuration guidance shall contain warnings about configuration accessible functions and privileges that should be controlled in a secure processing environment.**
AGD_OCD.1.4C	**The configuration guidance shall clearly present all configuration related responsibilities necessary for secure operation of the TOE.**
AGD_OCD.1.5C	**The user guidance shall be consistent with all other documentation supplied for evaluation.**
AGD_OCD.1.6C	**The configuration guidance shall describe all security requirements relative to the System environment.**
AGD_OCD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4 Life Cycle Support (ALC)

Identification of Security Measures (ALC_DVS.1)

Dependencies: No dependencies.

ALC_DVS.1.1D	**The developer shall produce development security documentation.**
ALC_DVS.1.1C	**The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.**
ALC_DVS.1.2C	**The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.**
ALC_DVS.1.1E	**The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**
ALC_DVS.1.2E	**The evaluator shall confirm tha the security measures are being applied.**

Systematic Flaw Remediation (ALC_FLR.3)

Dependencies:	No dependencies.
ALC_FLR.3.1D	The developer shall provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.3.2D	The developer shall establish a a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.3.3D	The developer shall provide remediation guidance addressed to TOE users.
ALC_FLR.3.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.3.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.3.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.3.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.3.5C	The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.3.6C	The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.3.7C	The procedures for processing reported security flaws shall provide safeguards that any correction to these security flaws do not introduce any new flaws.
ALC_FLR.3.8C	The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.3.9C	**The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of**

	security flaw reports and the associated corrections to registered users who might be affected by the security flaw.
ALC_FLR.3.10C	**The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security reports and corrections.**
ALC_FLR.3.11C	**The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.**
ALC_FLR.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Adequacy of Operational Security Measures (ALC_OPS.2)

Dependencies:	ASD_COM.1 Operational System Security Concept of Operations
ALC_OPS.2.1D	**The developer/integrator/system owner shall produce operations security documentation.**
ALC_OPS.2.1C	**The operations security documentation shall describe all the physical, procedural, personnel, and other security controls measures that are required to protect the integrity of the System TOE implementation in its operational environment.**
ALC_OPS2.2C	**The operations security documentation shall provide evidence that these security control measures are in place, followed, and enforced during the operations and maintenance of the System TOE.**
ALC_OPS.2.3C	**The evidence shall provide support that the security control measures, as implemented, provide the required level of protection to maintain effective security of the System TOE.**
ALC_OPS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_OPS.2.2E	The evaluator shall confirm that the security controls measures are being applied.

6.2.5 Security Awareness (ASA)

Verified Operational Security Guidance (ASA_PPG.2)

Dependencies:	No dependencies.
ASA_PPG.2.1D	**The system owner/management shall provide security policy and procedure guidance addressed to [selection: [assignment: *appropriate personnel definition*], *all*] personnel.**
ASA_PPG.2.1C	**The security policy and procedure guidance shall describe the security policies applicable to the system for the target personnel**
ASA_PPG.2.2C	**The security policy and procedure guidance shall describe how personnel can obtain the full contents of the security policies applicable to the system for the target personnel**
ASA_PPG.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASA_PPG.2.2E	**The evaluator shall independently verify through [selection: *personnel interviews, sampling the procedures in the security policy and procedure guidance*, [assignment: *other methods*]] the veracity of the contents of the security policy and procedures guidance.**

6.2.6 System O&M Security Controls (ASC)

Security Policy, Procedures and Organization (ASC_PPO.1)

Dependencies:	No dependencies.
ASC_PPO.1.1D	**The system owner shall provide operational security documentation.**
ASC_PPO.1.1C	**The security controls documentation shall describe all the policy, procedural, personnel, and related organisational security controls measures that are necessary to protect the confidentiality and integrity of the operations and maintenance of the System TOE in its operational environment.**
ASC_PPO.1.2C	**The operations security documentation shall provide evidence that these security controls measures are followed during the operation and maintenance of the System TOE.**
ASC_PPO.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASC_PPO.1.2E	**The evaluator shall confirm that the security controls are being applied.**

Physical, Facility and Assets (ASC_PFA.1)

Dependencies:	No dependencies.
ASC_PFA.1.1D	**The developer/system owner/integrator shall provide documentation for the physical, facility, and assets that comprise the System security controls.**
ASC_PFA.1.1C	**The security controls documentation shall describe all the physical, facility and assets related security controls measures that are necessary to protect the confidentiality and integrity of the operations and maintenance of the System TOE in its operational environment.**
ASC_PFA.1.2C	**The operations security documentation shall provide evidence that these physical security controls measures are followed during the operation and maintenance of the System TOE.**
ASC_PFA.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASC_PFA.1.2E	**The evaluator shall confirm that the physical security controls are being applied effectively.**

Operational Integration (ASC_OIN.1)

Dependencies:	No dependencies.
ASC_OIN.1.1D	**The developer/system owner/integrator shall provide operational security documentation.**
ASC_OIN.1.1C	**The operational system security documentation shall describe the integrated system security controls; to include IT and physical, policy, procedural, personnel, and other system security measures that are necessary to protect the confidentiality and integrity of the operations and maintenance of the System TOE in its operational environment.**
ASC_OIN.1.2C	**The operations security documentation shall provide evidence that the integrated security control measures are followed as part of the operations and maintenance of the System TOE.**
ASC_OIN.1.3C	**The evidence shall justify the integrated security measures provide**

	the necessary level of protection to maintain the confidentiality and integrity of the System TOE.
ASC_OIN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASC_OIN.1.2E	**The evaluator shall confirm that the integrated system security measures are being applied.**

6.2.7 System Architecture (Class ASD)

Operational System Architecture Design (ASD_SAD.1)

Dependencies:	No dependencies.
ASD_SAD.1.1D	**The developer/integrator shall provide an architecture description.**
ASD_SAD.1.1C	**The architecture description shall identify the system in terms of its subsystems and critical components and the interfaces and interconnects between the subsystems and critical components.**
ASD_SAD.1.2C	**The architecture description shall identify the super-systems that interact with the system and the interfaces and interconnects between the system and the super-systems.**
ASD_SAD.1.3C	**The architecture description shall describe the purpose of the identified subsystems, critical components, interconnects and interfaces of the system.**
ASD_SAD.1.4C	**The architecture description shall describe the purpose of the identified interconnects and interfaces from the system to super-systems and shall describe the services from and provided to the super-systems.**
ASD_SAD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASD_SAD.1.2E	**The evaluator shall determine that the architecture description is consistent with the interface functional specification.**

Operational System Interface Functional Specification (ASD_IFS.1)

Dependencies:	No dependencies.
ASD_IFS.1.1D	**The developer/integrator shall provide an interface functional specification.**
ASD_IFS.1.1C	**The interface functional specification shall describe the operational system security functions.**
ASD_IFS.1.2C	**The interfaces functional specification shall be internally consistent.**
ASD_IFS.1.3C	**The interface functional specification shall identify and describe all the external system security function interfaces, including the behaviour of those interfaces.**
ASD_IFS.1.4C	**The interface functional specification shall cover all the system security functions.**
ASD_IFS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASD_IFS.1.2E	**The evaluator shall determine whether the interface functional specification is a complete instantiation of the system security functional requirements.**

Subsystem Design Allocation (ASD_SSD.2)

Dependencies:	ASD_SSD.1 Subsystem design.
ASD_SSD.2.1D	**The developer/integrator shall provide a subsystem design.**
ASD_SSD.2.1C	**The subsystem design shall be internally consistent.**
ASD_SSD.2.2C	**The subsystem design shall allocate the portion of the SSF to each represented subsystem in terms of minor and major subsystems.**
ASD_SSD.2.3C	**The subsystem design shall describe the security functionality provided by each subsystem.**
ASD_SSD.2.4C	**The subsystem design shall identify all hardware, firmware, and software required by the SSF allocated to the subsystem.**
ASD_SSD.2.5C	**The subsystem design shall allocate the portion of the SSF to each**

	represented subsystem in terms of minor and major subsystems.
ASD_SSD.2.6C	**The subsystem design shall identify the interfaces to the subsystem security functions**.
ASD_SSD.2.7C	**The subsystem design shall describe the interfaces to each subsystem, in terms of their purpose and method of use of the effects, exceptions and error messages.**
ASD_SSD.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASD_SSD.2.2E	**The evaluator shall determine whether the subsystem design is a complete instantiation of the operational system security functional requirements.**

Implementation Representation (ASD_IMP.1)

Dependencies:	No dependencies..
ASD_IMP.1.1D	**The developer/integrator shall provide an implementation representation of the system design.**
ASD_IMP.1.1C	**The implementation representation shall be internally consistent.**
ASD_IMP.1.2C	**The implementation representation identify the system functionality, and the system components that when integrated provide that functionality to the operational system.**
ASD_IMP.1.3C	**The implementation representation shall describe the security functionality provided by the integration of each component in terms of its specific configuration requirements.**
ASD_IMP.1.4C	**The implementation representation shall identify any hardware, firmware, and software integration and configuration issues, as identified, prior to, or during the operational system evaluation, that will need to be revisited.**
ASD_IMP.1.5C	**The implementation representation shall identify the integrated components and their required configuration to the system security functions**.
ASD_IMP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASD_IMP.1.2E	**The evaluator shall determine whether the implementation representation is a complete instantiation of the integrated operational system security functional requirements.**

Operational System Security Concept of Operations (ASD_COM.1)

Dependencies:	No dependencies.
ASD_COM.1.1D	**The system owner/management shall provide a system operations policy documents.**
ASD_COM.1.2D	**The system owner/integrator shall incorporate system policy enforcement requirements and capabilities into the policy documents provided by the system management, and provide the system operations policy documents with the system enforcement capabilities, and their bounds.**
ASD_COM.1.1C	**The system concept of operations and enforcement documents subsystem shall be internally consistent.**
ASD_COM.1.2C	**The operational system operations policy documents shall identify the system capabilities for enforcement of information flow across the operational system interconnects within the operational system boundaries.**
ASD_COM.1.3C	**The operational system operations policy documents shall identify the system capabilities for enforcement of information flow across the operational system interconnects to external operational systems.**
ASD_COM.1.4C	**The operational system operations policy documents shall identify the system capabilities for enforcement of local and remote access to the operational system.**
ASD_COM.1.5C	**The operational system operations policy documents shall identify the system capabilities for enforcement of access to operational system resources based upon access mediation rules.**
ASD_COM.1.6C	**The operational system operations policy documents shall identify the modes of operation provided by the system, and the enforcement mechanisms to provide secure operations in each of the identified system modes of operation.**
ASD_SSD.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASD_SSD.2.2E	**The evaluator shall determine whether the system design is a complete instantiation of the operational system security concept of operations in support of the operational mission.**

6.2.8 Tests (ATE)

System Security Controls Testing (ATE_AST.3)

Dependencies:	AGD_OCD.1 System operational configuration definition. AGD_USR.1 ASD_IFS.1 System interface functional definition ASD_IMP.1 Implementation representation
ATE_AST.3.1D	**The developer/integrator shall provide evidence of test verification planning.**
ATE_AST.3.2D	**The developer/integrator shall provide an analysis of level of detail of integrated security controls testing.**
ATE_AST.3.3D	**The developer shall provide test documentation and the the System TOE for testing.**
ATE_AST.3.1C	**The analysis of the security controls verification shall demonstrate that the correspondence between the security controls as identified in the SST and the tests identified in the test documentation is complete.**
ATE_AST.3.2C	**The level of detail analysis shall show that the integrated security controls tests identified in the test documentation are able to sufficiently demonstrate that the system security controls integrated into the System TSF operates in accordance with its high level design.**
ATE_AST.3.3C	**The level of detail analysis shall show that the integrated security controls tests identified in the test documentation are able to sufficiently demonstrate that the system security controls integrated into the System TSF; and are a correct implementation.**
ATE_AST.3.4C	**The System TOE shall be suitable for testing.**
ATE_AST.3.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_AST.3.2E	**The evaluator shall test a subset of the system TSF to confirm that the system TOE operates as specified in its intended operational**

environment.

Functional Testing (ATE_FUN.1)

Dependencies:	No dependencies.
ATE_FUN.1.1D	**The developer/integrator shall test the TSF and documents the results.**
ATE_FUN.1.2D	**The developer/integrator shall provide test documentation.**
ATE_FUN.1.1C	**The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.**
ATE_FUN.1.2C	**The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.**
ATE_FUN.1.3C	**The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.**
ATE_FUN.1.4C	**The expected test results shall show the anticipated outputs from a successful execution of the tests.**
ATE_FUN.1.5C	**The test results from the developer/integrator execution of the tests shall demonstrate that each test security function behaved as specified.**
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.9 Vulnerability Assessment (AVA)

6.2.10 Assurance Maintenance (AMA)

Assurance Maintenance (AMA_AMP.1)

Dependencies:	No dependencies.
AMA_AMP.1.1D	**The developer/integrator shall provide an AM Plan.**
AMA_AMP.1.1C	**The AM Plan shall contain or reference a brief description of the TOE including the security functionality it provides.**
AMA_AMP.1.2C	**The AM Plan shall identify the certified version of the system TOE, and shall reference the evaluation results..**
AMA_AMP.1.3C	**The AM Plan shall reference the TOE component categorization report for the certified version of the TOE.**
AMA_AMP.1.4C	**The AM Plan shall define the scope of changes to the STOE that are covered by the plan.**
AMA_AMP.1.5C	**The AM Plan shall describe the TOE life-cycle, and shall identify the current plans for any new releases of the TOE, together with a brief description of any planned changes that are likely to have a significant security impact.**
AMA_AMP.1.6C	**The AM Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule of AM audits and the target date of the next re-evaluation of the TOE.**
AMA_AMP.1.7C	**The AM Plan shall identify the individual(s) who will assume the role of developer/system owner security analyst for the system TOE.**
AMA_AMP.1.8C	**The AM Plan shall describe how the developer/system owner security analyst role will ensure that the procedures documented or referenced in the AM Plan are followed.**
AMA_AMP.1.9C	**The AM Plan shall describe how the developer/system owner security analyst role will ensure that all developer/integrator actions involved in the analysis of the security impact of changes affecting the TOE are performed correctly.**
AMA_AMP.1.10C	**The AM Plan shall justify why the identified developer/system owner security analyst(s) have sufficient familiarity with the security target, functional specification and (where appropriate) high level design of the TOE, and with the evaluation results and all applicable assurance requirements for the certified version of the TOE.**
AMA_AMP.1.11C	**The AM Plan shall describe or reference the procedures to be applied to maintain the assurance in the TOE, which shall include the**

	procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the TOE, and flaw remediation.
AMA_AMP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AMA_AMP.1.2E	The evaluator shall confirm that the proposed schedules for AM audits and re-evaluation of the TOE are acceptable and consistent with the proposed changes to the TOE.

6.3 Security Requirements for the IT Environment

The STOE has no requirements for the external IT environment, other than those stipulated by the organizational security policies (refer to section 3.3).

6.4 Security Requirements for the Non-IT Environment

The STOE has no requirements for the external non-IT environment, other than those stipulated by the organizational security policies (refer to section 3.3).

7 SPP Application Notes

Editor's note: To be completed in the next release. Overall structure of chapter provided for comment.

This section of the document contains supporting information that will be useful in developing more focused system protection profiles or security targets for specific classes of industrial control systems, for example SCADA systems, or for specific applications of industrial control systems.

7.1 SPP Overview

7.1.1 SPP Purpose

A system protection profile provides a statement of the security requirements, generally at an abstract / implementation independent level but can provide industry specific implementation details to ensure consistent compliance.

Therefore, for a specific community of interest (e.g. the process control industry) providing a related family of "constructs" (i.e. system protection profiles, functional packages, assurance packages, system security targets) that help to ensure interoperability, provide for a consistent implementation of security controls, countermeasures and ensures sufficient assurance (confidence in the ultimate system).

The following diagram illustrates how the Application Notes will eventually provide the required guidance on how to develop, and the relationships amongst the family of "constructs" being developed to support the ICS.

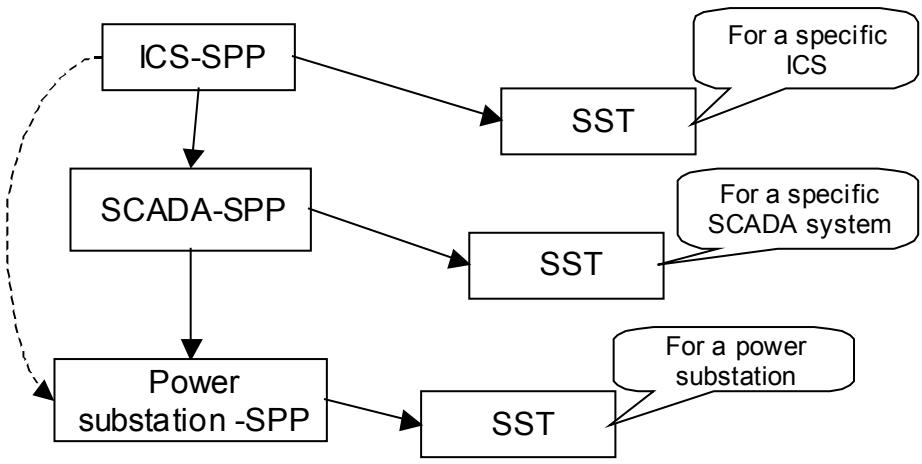

Figure 3 - Relationship between ICS-SPP and other potential SPP's and SST's

7.1.2 SPP Structure

- SPP structure flowchart
- SPP concept relationships
- Integration of risk
- Importance of risk management

7.1.3 SPP Application

- Intended application
- Application of the ICS-SPP to specific ICS' requirements (e.g. SCADA)
- Completing the SPP for other uses

7.2 SPP Application: System Requirements Specification

7.2.1 Traditional CC Paradigm

- Technical nature of TOE Security Functions (TSF)

7.2.2 Systems Context

- The need for System Security Functions (SSF)
- Technical Security Functions (TSF)
- Policy, Procedural and Physical Functions (PSF)

7.3 SPP Application: Risk Management

- Importance of risk management
- Overview of the risk management process (based on the newly revised NIST Special Publication 800-30)
- Integration of the risk management process with the ICS-SPP
    - Context Establishment
    - Risk Identification
    - Risk Analysis (including threat assessment & vulnerability assessment)
    - Risk Evaluation
    - Risk Treatment
    - Risk Monitoring

7.4 SPP Application: SPP

This section provides guidance on how to refine the ICS-SPP into further SPP's for specific ICS systems (e.g. SCADA systems).

7.4.1 Refinement of the Security Environment

7.4.1.1 Assumptions, Threats and OOSPs

- Additions
- Modifications

- Deletions

7.4.1.2 System Assets

- Identification of critical assets

7.4.1.3 Vulnerability Analysis

- Integration with the security environment
- Refinement during the STOE evaluation

7.4.1.4 Threat Analysis

- Integration with the security environment
- Refinement during the STOE evaluation

7.4.2 Risks

7.4.2.1 Identification of Additional Risks to the System

- Technical controls
- Management controls
- Operational controls

7.4.2.2 Refinement of Identified Risks

- Additions
- Modifications
- Deletions

7.4.3 Refinement of the Security Objectives

- Additions
- Modifications
- Deletions

7.4.4 Refinement of the IT Security Requirements

7.4.4.1 Integration of level of risk to the Functional Security Requirements

7.4.4.2 Integration of level of risk to the Assurance Security Requirements

7.4.5 Supporting Rationale

7.4.5.1 Security Risks Rationale

- Mapping assets, threats and vulnerabilities to identified risks
- Sufficiency of security risks

7.4.5.2 Security Objectives Rationale

- Suitability of the security objectives to counter identified risks
- Sufficiency of the security objectives to counter identified risks

7.5 SPP Application: SST

This section provides guidance on how to claim conformance to the ICS-SPP for specific ICS systems.

7.5.1 STOE Summary Specification

7.5.1.1 Selection of Controls

- Management
- Operational
- Technical

7.5.1.2 Mitigation of the Risk

- Risk Treatment: avoidance, reduction of likelihood, reduction of impact, risk transference and risk retention.
- Risk Monitoring: risk management plan

7.5.2 SPP Claims

7.5.2.1 Conformance to the ICS-SPP

7.5.3 Supporting Rationale

7.5.3.1 Sufficiency of Controls to meet the Security Objectives

7.5.3.2 Sufficiency of Controls to mitigate the Identified Risks

8 Rationale

Editor's note: To be completed in the next release.

8.1 Security Risks Rationale

The purpose of this rationale is to demonstrate that the identified security risks are suitable, that is they are sufficient to address the security needs, and that they are necessary, ie, there are no redundant security risks.

8.1.1 All Assets, Threats and Vulnerabilities Addressed

The need to demonstrate that there are no redundant security risks is satisfied as follows:

- The first section (Table 14) shows that all of the assets, threats to security, and vulnerabilities have been addressed.
- The second section (Table 15) shows that each security risk addresses at least one assumption, policy, and threat combination.

Table 14 - Mapping of Assets, Threats and Vulnerabilities to Security Risks

Asset/Threat/Vulnerability Label	Associated Security Risk
A.	OE.
T.	O.
P.	O.

Table 15 shows that there are no unnecessary IT security risks.

Table 15 - Mapping of Security Risks to Assets, Threats and Vulnerabilities

Risk Label	Asset / Threat/ Vulnerability
R.	ASSET. T. V.
R.	ASSET. T. V.
R.	ASSET. T. V.

8.1.2 Security Risks are Sufficient

The following arguments are provided in Table 16 to demonstrate the sufficiency of the Security Risks outlined above.

Table 16 - Sufficiency of Security Risks

Asset/Threat/Vulnerability	Argument to support Security Risk sufficiency
A.	
T.	
V.	

8.2 Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are suitable, that is they are sufficient to address the security needs, and that they are necessary, ie, there are no redundant security objectives.

8.2.1 All Assumptions, Threats and Policies Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section (Table 17) shows that all of the secure usage assumptions, threats to security, and organizational security policies have been addressed.
- The second section (Table 18) shows that each security objective counters at least one assumption, policy, or threat.

Table 17 - Mapping of Assumptions, Threats, and OSPs to Security Objectives

Threat/Policy/Assumption Label	Associated Security Objective
A.	OE.
T.	O.
P.	O.

Table 18 shows that there are no unnecessary IT security objectives.

Table 18 - Mapping of Security Objectives to Threats, Policies and Assumptions

Objective Label	Threat / Policy/ Assumption
O.	A. T. P.
O.	A. T. P.
O.	A. T. P.

8.2.2 Security Objectives are Sufficient

The following arguments are provided in Table 19 to demonstrate the sufficiency of the Security Objectives outlined above.

Table 19 - Sufficiency of Security Objectives

Assumption/Threat/Policy	Argument to support Security Objective sufficiency
A.	
T.	
P.	

8.2.3 Suitability of the Security Objectives to counter identified Risks

The purpose of this section is to show that the security objectives are suitable to address the identified security risks. Table 20 and Table 21 show that each security objective is necessary, that is, each security risk is addressed by at least one security objective and vice versa.

Table 20 - Mapping of Security Risks to Security Objectives

Security Risks	Security Objectives
R.	O.
R.	O.
R.	O.

Table 21 - Mapping of Security Objectives to Security Risks

Security Objective	Security Risk
O.	R.
O.	R.
O.	R.

8.2.4 Sufficiency of the Security Objectives to counter identified Risks

The following table shows that security objectives are sufficient to counter the security risks, whether in a principal or supporting role.

Table 22 - Sufficiency of Security Objectives countering identified Risks

Security Risks	Argument to support sufficiency of Security Objectives countering identified Risks
R.	
R.	

R.	

8.3 Security Requirements Rationale

8.3.1 Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are suitable to meet the security objectives. Table 23 and Table 24 show that each security requirement is necessary, that is, each security objective is addressed by at least one security requirement and vice versa. Note that some objectives are partially satisfied by the STOE and partially satisfied by the IT environment. Security Objectives for the STOE are satisfied by Common Criteria functional components. Security Objectives for the Environment are satisfied by IT requirements for the environment.

Table 23 - Mapping of Security Objectives to Security Requirements

Security Objectives	Security Requirements
O.	F
O.	F
O.	F

Table 24 - Mapping of Security Requirements to Security Objectives

Requirements	Objective
F	O.
F	O.
F	O.

8.3.2 Sufficiency of the Security Requirements

The following table shows that security requirements are sufficient to satisfy the STOE security objectives, whether in a principal or supporting role.

Table 25 - Sufficiency of Security Requirements

Objectives	Argument to support sufficiency of Security Requirements
O.	
O.	
O.	

8.3.3 Satisfaction of Dependencies

Table 26 shows the dependencies between the functional requirements. All of the dependencies are satisfied. Note that:

(H) indicates the dependency is satisfied through the inclusion of a component that is hierarchical to the one required).

(*) indicates that this dependency is not satisfied by the TOE. Refer to the supporting rationale following Table 26.

Table 26 - Dependency Analysis

Component Reference Dependency Reference	Requirement	Dependencies	
Functional Requirements			
1	FAU_ARP.1	FAU_SAA.1	
Assurance Requirements			
8	ACM_CAP.2	None	-
9	ADO_DEL.1	None	-
10	ADO_IGS.1	AGD_ADM.1	
11	ADV_FSP.1	ADV_RCR.1	
12	ADV_HLD.1	ADV_FSP.1, ADV_RCR.1	
13	ADV_RCR.1	None	-
14	ADV_SPM.1	ADV_FSP.1	
15	AGD_ADM.1	ADV_FSP.1	
16	AGD_USR.1	ADV_FSP.1	
17	ATE_COV.1	ADV_FSP.1, ATE_FUN.1	

18	ATE_FUN.1	None	-
19	ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	
20	AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	
21	AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1	

The following dependencies are not satisfied in this System Protection Profile because they are not considered relevant to the STOE for the provided reasons:

- TBD

8.4 Rationale for Extensions

TBD

Appendix A – Acronyms

Editor's note: To be completed in next release.

CC	Common Criteria
EAL	Evaluation Assurance Level
ICS	Industrial Control System
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PP	Protection Profile
PSF	Procedural, Policy, Personnel & Physical Security Functions
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SPP	System Protection Profile
ST	Security Target
SST	System Security Target
STOE	System Target of Evaluation
TSC	TSF Scope of Control
TSF	Technical Security Functions
SSF	System Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy